REMARKS/ARGUMENTS

Claims 1-5, 7-9, 12, 14, and 23-33 are pending in the present application. Claims 1, 12, 23, 27, and 33 were amended. Claims 34 and 35 are added. Claims 5 and 13 are cancelled. Support for the amendments and newly added claims can be found in the Specification at least on page 1, lines 5-7, page 6, lines 5-20, page 8, lines 17-22, Figure 1 and Figure 2. Reconsideration of the claims is respectfully requested.

I. Examiner Interview

Applicants thank Examiner Zia for all the courtesies extended Applicants' representative during the February 23, 2006 telephone interview. During the interview, Applicants' representative discussed the prior art of record and the manner in which the present invention in independent claims 1 and 23 are distinguishable over *Liao*. The Examiner agreed to consider Applicant's arguments and amendments when submitted. The arguments discussed as well as additional reasons that the claims are not anticipated are set forth in the remarks below.

II. 35 U.S.C. § 102, Anticipation: Claims 1-5, 7-9, 12-14, and 23-33

The examiner has rejected claims 1-5, 7-9, 12-14, and 23-33 under 35 U.S.C. § 102(e) as being anticipated by Liao et al., Method and System for Secure Lightweight Transactions in Wireless Data Networks, U.S. Patent No. 6,480,957, November 12, 2002* (hereinafter "*Liao*"). This rejection is respectfully traversed.

Independent Claim 1

The examiner states on pages 3-6 of the Office Action dated December 14, 2005 that:

> 1. Regarding Claim 1 Liao teach and describe a method for controlling access to protected contents on. a server, the method requiring the following components to be present (Fig.1-7):
> a) a server, b) a client, c) a reader for a mobile security module, d) a security module having at least one protected area for storing a key, e) a data line for communications between client and server (Fig.1, and col.5 line 53 to col. 7 line 12), characterized by the following steps:
> aa) sending to the server of a request to call up protected-access contents, bb) sending from the server to the client of an authentication module to be run in the client, cc) execution of an authentication protocol

* This patent is subject to a terminal disclaimer

> for authenticating the mobile security module and, where appropriate, its holder by means of the authentication module, dd) if the authentication in step cc) was successful, addition to the request in step aa) of a session ID which was generated in the course of the communications between the authentication module and the server, ee) sending of the new request to the server application, ff) checking of the session ID in the request to see that it is recorded in the server, gg) processing of the content requested for transmission and searching of. the contents for further links to other protected-access contents, hh) addition of the session){D to the links identified, ii) sending of the content modified as in step hh) to the client (Fig.1, 4-7, and col.7 line 13 to line 32, and col.11 line Ito col.13 line 62).

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. In re Bond, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. In re Lowry, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. Kalman v. Kimberly-Clark Corp., 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). In this case, *Chen* does not identically show each and every feature of the claims arranged as they are in the claims.

Amended independent claim 1 recites as follows:

> 1. A computer implemented method for controlling access to protected contents on a server using a mobile security module, the computer implemented method requiring the following components to be present:
>
> a) a server;
>
> b) a client;
>
> c) a reader for a mobile security module;
>
> d) a mobile security module associated with the client and having at least one protected area for storing a key; and
>
> e) a data line for communications between client and server; and
>
> wherein the computer implemented method comprises the following steps:
>
> aa) sending to the server of a request to call up protected-access contents;
>
> bb) sending from the server to the client of an authentication module to be run in the client;
>
> cc) execution of an authentication protocol for authenticating the mobile security module and, where appropriate, its holder by means of the authentication module;

dd) if the authentication in step cc) was successful, addition to the request in step aa) of a session ID which was generated in the course of the communications between the authentication module and the server;

ee) sending of the new request to the server application;

ff) checking of the session ID in the request to see that it is recorded in the server;

gg) processing of the content requested for transmission and searching of the contents for further links to other protected-access contents;

hh) addition of the session ID to the links identified; and

ii) sending of the content modified as in step hh) to the client.

Liao does not teach the feature of a mobile security module or the steps of execution of an authentication protocol or searching of the contents for further links as recited in independent claim 1.

1. **A mobile security module**

Liao does not teach "a mobile security module associated with the client and having at least one protected area for storing a key," as is recited in independent claim 1. The Examiner believes this feature is taught by *Liao* at Figure 1 and column 5, line 53 to column 7, line 12. Figure 1 of *Liao* illustrates as follows:

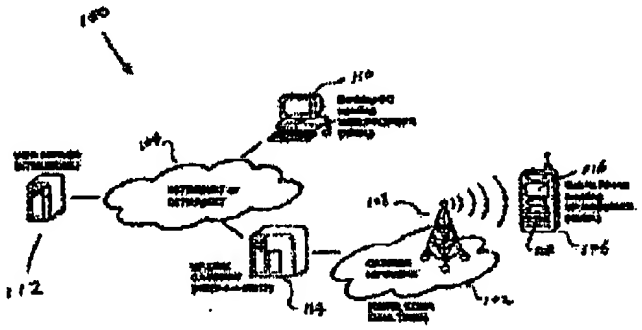


Fig. 1

Liao, Figure 1.

Here, *Liao* illustrates a wireless data network that includes a desktop PC running a web browser, a web server, an internet or intranet connection, a link server, a carrier network, and a mobile phone. However, as can be seen, Figure 1 does not depict or disclose a mobile security module.

Liao at column 5, line 53 to column 6, line 53, which is cited by the Examiner, describes Figure 1 as follows:

Referring now to the drawings, in which like numerals refer to like parts throughout the several views. FIG. 1 shows a schematic representation of a wireless data network 100 in which the present invention may be practiced. The data network 100 comprises an airnet 102 and the landline network 104, each acting as a communication medium for data transmission therethrough. The landline network 104 may be the Internet, the Intranet or other private networks. For simplicity, the landline network 104 will be herein simply referred to as the Internet, literally meaning either the Internet or the Intranet or other private network. Further the airnet 102, an meaning an unwired network in which data transmission is via the air, is sometimes referred to as a carrier network because each airnet is controlled and operated by a carrier, for example AT&T and GTE, each having its own communication scheme, such as CDPD, CDMA, GSM and TDMA. Referenced by 106 is a mobile data device, but resembling a mobile phone, in communication with the airnet 102 via an antenna 108. It is generally understood that the airnet 102 communicates simultaneously with a plurality of mobile computing devices of which a mobile phone 106 is shown in the figure. Similarly connected to the Internet 104 are a plurality of desktop PCs 110 and a plurality of web servers 112, though only one representative respectively shown in the figure. The PC 110, as shown in the figure, may be a personal computer SPL 300 from NEC Technologies Inc. and runs a web browser via the Internet 104 to access information stored in the web server 112 that may be a workstation from SUN Microsystems Inc. It is understood to those skilled in the art that the PC 110 can store accessible information so as to become a web server as well. Between the Internet 104 and the airnet 102 there is a link server 114 performing data communication between the Internet 104 and the airnet 102. The link server 114, also referred to as link proxy or gateway, may be a workstation or a personal computer and performs a protocol mapping from one communication protocol to another, thereby a mobile device 106 can be in communication with any one of the web servers 112 or the PCs 110, respectively.

The communication protocol in the Internet 104 is HTTP that runs on TCP and controls the connection of an HTML Web browser to a Web server and the exchange of information therebetween. An extended version thereof, called HTTPS, provides encrypted authentication and session transmission between a client and a server. The communication protocol between the mobile device 106 and the link server 114 via the airnet 102 is Handheld Device Transport Protocol (HDTP), or Secure Uplink Gateway Protocol (SUGP), which preferably runs on User Datagram Protocol (UDP) and controls the connection of a HDML Web browser to a link server, where HDML stands for HandHeld Markup Language. The specification thereof and the HDTP specification are provided at http://www.wapforum.org http://www.openwave.com that are incorporated herein by reference. Further a reference specification entitled "Magellan SUGP Protocol" is incorporated herein by reference. The HDTP is a session-level protocol that resembles the HTTP but without incurring the overhead thereof and is highly optimized for use in mobile devices that have significantly less computing power and memory. Further it is understood to those skilled in the art that the UDP does not require a connection to be established between a client and a server before

> information can be exchanged, which eliminates the need of exchanging a large number of packets during a session creation. Exchanging a very small number of packets during a transaction is one of the desirous features for a mobile device with very limited computing power and memory to effectively interact with a landline device.

Liao, column 5, line 53 to column 6, line 53.

This portion of *Liao* describes a wireless data network that includes an airnet and a landline network acting as a communication medium for data transmission. The landline network can be the Internet, an intranet, or private network. The airnet communicates with mobile computing devices, such as a mobile phone. Desktop PCs and web servers may also be connected to the Internet. *Liao* also discusses the HTTP communication protocol for the Internet. Although *Liao* mentions mobile computing devices, *Liao* does not teach a **mobile security module.** Furthermore, this portion of *Liao* does not teach or mention a security module of any kind having a protected area for storing a key.

The next portion of the reference cited by the Examiner at column 6, line 54 to column 7, line 12 states as follows:

> According to one preferred embodiment, the present invention may be practiced with a cellular phone, a typical example of the mobile device 106, that has very limited computing power and memory. The cellular phone 106 is used as a client in communication to a landline device that is often referred to as a server providing accessible information therein to other devices. FIG. 2 shows a block diagram of a typical GSM digital cellular phone 120. Each of the hardware components in the cellular phone 120 is known to those skilled in the art and so the hardware components are not to be described in detail herein. Although the user interface of the phone 120 is not shown in the figure, the mobile device 118, resembling a cellular phone, in FIG. 1 may be referenced thereto, in which referenced by 116 is a LCD screen and 118 is a key button pad, respectively. Through the screen 116 and the keypad 118 controlled by a user of the phone, the phone can be interactively communicated with a server through the airnet, link server and the Internet. According to one embodiment of the present invention, compiled and linked processes of the present invention are stored in ROM 122 as a client module 124 and support module 126. Upon activation of a predetermined key sequence utilizing the keypad 118, a physical layer processor or microcontroller 118, initiates a session communication to the server using the module 124 in the ROM 122.

Liao at column 6, line 54 to column 7, line 12.

In this portion of the reference *Liao* describes the wireless data network depicted in Figure 1. As previously discussed, *Liao* merely discloses a network that includes an airnet, a landline network, a mobile data device such as a mobile phone, a personal computer, web servers, a link server, and various other components of a wireless network. Although *Liao* discloses a mobile data device or mobile phone, such teachings do not disclose a mobile security module that has a protected area for storing a key. In fact, *Liao* does not disclose or even mention a mobile security module, a protected area, or storing a key in this or any other section of the reference. Thus, *Liao* does not disclose "a mobile security module having at least one protected area for storing a key, wherein the mobile security module is a chip card," as is recited in amended claim 1.

2. Execution of an authentication protocol

Liao does not teach "execution of an authentication protocol for authenticating the mobile security module and, where appropriate, its holder by means of the authentication module," as is recited in amended claim 1. The Examiner alleges that this step is disclosed in *Liao* at Figs. 1, 4-7, and column 7, lines 13-32, and column 11, line 1 to column 13, line 62. As shown above, Figure 1 does not disclose a mobile security module. Furthermore, Figure 1 does not illustrate or disclose execution of an authentication protocol or authenticating a mobile security module by means of an authentication module.

The cited portion of *Liao* at column 7, lines 13-32 states as follows:

> To establish a secured communication between a client and a server, an authentication process must be conducted first to ensure that only interested parties are actually in the communication therebetween. The process is complete through two rounds of independent authentication, one being the client authenticated by the server, referred to as client authentication, and the other being the server authenticated by the client, referred to as server authentication. Further each authentication is completed in two separate steps for high grade of security, which will be described in detail below. The success of the mutual authentication processes provision an evidence that the two communicating parties possesses a valid shared secret encrypt key through a mutual decryption and a challenge/response mechanism. The mutual decryption mechanism comprises the steps of mutually recovering encrypted messages from two involved communicating parties. The challenge/response mechanism, referred to as nonce verification, verifies a predetermined relationship between a sent nonce and a received derivative thereof.

Liao, column 7, lines 13-32.

Here, *Liao* teaches an authentication process is conducted to ensure only interested parties are in a communication. The authentication process involves two rounds of authentication in which both a server is authenticated and a client is authenticated. Thus, *Liao* merely teaches an authentication process between a server and client that involves utilization of a shared secret encrypt key. However, *Liao* does not teach a mobile security module, or an authentication process for authenticating a mobile security module means of an authentication module sent to a client by a server in this or any other section of the reference.

Figure 4a of *Liao* illustrates as follows:

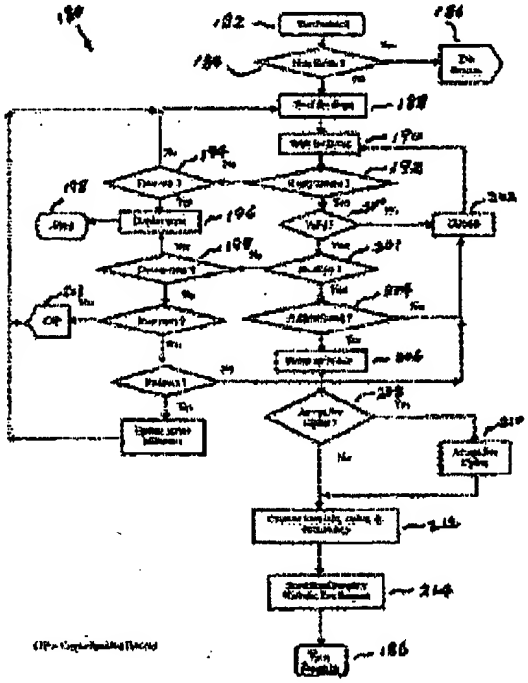


Fig. 4a

As shown above, Figure 4a depicts a flowchart illustrating a session creation process in which a client sends a session request "SessRqst", authenticates a session reply "SessRply", and sends a session complete "SessComplete". The flowchart does not depict any steps for authenticating a mobile security module by an authentication module. Although *Liao* authenticates a session reply, such an authentication step does not teach authenticating a mobile security module. Therefore, Figure 4a is insufficient to teach executing an authentication protocol for authenticating a mobile security module.

Figure 4b of *Liao* shows as follows:

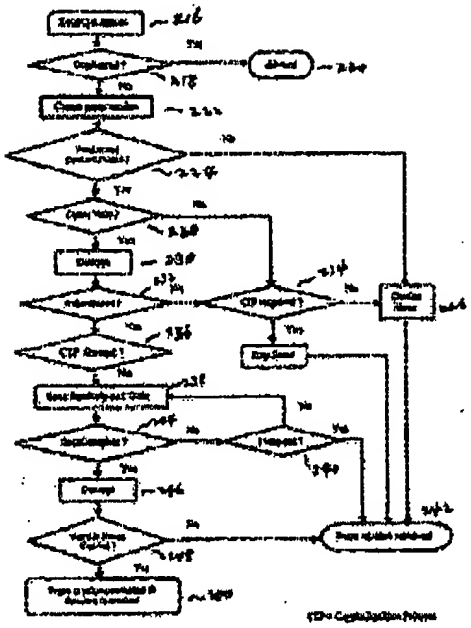


Fig. 4.b

Liao, Figure 4b.

Here, *Liao* illustrates another flowchart depicting a session creation process. The flowchart shows a session request "SessRqst" arrives, validates the session request to authenticate the client, sends a session reply "SessRply", and validates a session complete "SessComplete". Although the flowchart shows steps for validating a session request signal and validating a session complete signal to authenticate a client, the flowchart does not depict steps for authenticating a mobile security module.

The portion of *Liao* at column 11, lines 1-61, which is cited by the Examiner, teaches:

> Referring now to FIG. 4.a and FIG. 4.b, there are shown two data flowcharts 180 and 181 representing a session creation process in the client and the server, respectively, in one embodiment of the present invention. There are generally three types of transactions that are conducted between a mobile device and a landline server; service transaction, notification transaction, and post transaction. Both service and post transactions are initiated by the mobile device that is considered as a client herein and the notification transaction is initiated by the landline server that is considered a server herein. All transactions must be conducted in the context of a valid and established session. If there is no session

> or valid session, a session must be created before any transaction can start. For the sake of simplicity, it is assumed that the transaction is initiated at the client side at 182. As described above, for a transaction to take place in a secure communication, a session between a client and a server must be established first. Therefore at 184, the existence of a valid session is examined. If a valid session is in place, the transaction can proceed at 186. If there is no established session, for example, a mobile device is just powered on for the first time or a previous session is beyond a time limit, for example 8 hours, a session request must be initiated and sent to the server at 188. The client is then in a mode of waiting for a reply from the server, constantly looking up for the reply at 190 and 192. If there is no reply from the server, the client may initiate another session request if a fixed time period lapses at 194 or errors occur to have to abort the initiated session request at 196 and 198. The errors occur when the client is out of a service area covered by an airnet that communicates with the server or simply either the client or the server malfunctions at 199.
>
> Meanwhile the session request is received by the server at 216. A proto session is created at 222 per the session request from the client if the session request is not a duplicated one. It is very common that a session request may be retransmitted or re-requested by the client due to some unexpected error conditions in the wireless data network so that duplicated requests may be received. The server, however, uses a tag, which is generated from the encrypted message in the session request first received and is unique for each session request from a particular client, to prevent creating multiple proto sessions from the duplicated session requests. Some of the information in the session request, such as protocol version and device ID are verified at 224. If the verified information is not supported, there might be device error at 226, which results in the removal of the proto session just created. If the verifying process at 224 succeeds, the server proceeds a decryption process, according to a shared secret encrypt key as described above, to decrypt the C-nonce and C-nonceModified at 230. If the operational relationship between the C-nonce and C-nonceModified holds at the server side, the step one client authentication completes. CIP at 203 in FIG. 4.a and 234 and 236 of FIG. 4.b stands for crypto ignition process which is a process to equip a client with a updated encrypt information, for example, to update the share secret key. As the CIP is an added process and not a key element in the present invention, and no detail description thereof is provided therefore. With the successful step one client authentication, the server at 238 sends a session reply to the client.

Liao at column 11, lines 1-61.

Here, *Liao* describes a session creation process in a client and server in which transactions are initiated by a mobile device. A client sends a session request to a server to initiate a session creation. The server receives the session request and creates a protosession. The server verifies information in the session request, such as protocol version and device ID.

The server uses a shared secret encrypt key for a decryption process to authenticate the client. The server then sends a session reply to the client. However, this section of *Liao* does not teach authenticating or validating a mobile security module associated with a client. Moreover, the teaching of *Liao* regarding authenticating a client using a shared secret encrypt key is not sufficient to teach execution of an authentication protocol to authenticate a mobile security module.

The cited portion of *Liao* at column 11, line 62-column 12, line 35 teaches:

> When a server is reached and successfully processes the session request from the client, namely the step one client authentication as described above, a session reply is sent by the server to the client to start server authentication at the client side. Upon receiving the session reply from the server being connected, the client examines the reply signal at 200 and 201 and the session reply should be in a recognized format, such as uncorrupted essential information therein. If the received session reply is not recognized or supported, the client discards the received session reply at 202 and continues to wait for a valid session reply, otherwise problems with devices may be claimed in step 199. Upon receiving the session reply from the server, the client proceeds two steps of the server authentication at 204, which has been described above in detail. Logically the session is discarded at 202 if the server authentication fails, namely the client fails to decrypt and verify the encrypted S-nonce and to validate the derivative of the C-nonce generated by the server. When the server authentication passes, the client chooses either its own cipher or the server proposed cipher obtained from the session reply from the server at 208 and 210 and further the client retrieves the session key therefrom and sends a session complete signal to the server to complete the session creation at 212 and 214.
>
> Meanwhile the server expects a session complete signal from the client it just sends the session reply to at 238. For security purpose, the server drops the proto session at 242 if the time waiting for the session complete signal goes beyond a threshold 240. Upon receiving the session complete signal at 244, the server proceeds the step two client authentication at 246 and 248 by decrypting the encrypted derivative of the S-nonce and verifying the relationship thereof with the original S-nonce. If the decryption of the derivation or the verification with the S-nonce fails, the session creation fails, hence the removal of the proto session. If the step two client authentication succeeds, that means the step one client authentication and the step one and two server authentication have all completed, the session is successfully created by promoting the proto session to the regular session at 250, thereby the transaction originally initiated by the client at 182 of FIG. 4.a can proceed therefrom.

Liao, column 11, line 62-column 12, line 35.

This portion of the text cited by the Examiner describes a step in which a session reply is sent by a server to a client to start a server authentication at the client side. The client determines if the session reply is in a recognized format, performs a decryption process, chooses a cipher or chooses the server proposed cipher obtained from the session reply, retrieves a session key from the reply, and sends a session complete signal to the server. Upon receiving the session complete signal, the server performs a decryption process to authenticate the client. If the authentication is successful, the protosession is promoted to a regular session. Once again, *Liao* merely discusses a two step authentication process for authenticating a server by a client and authenticating a client by a server. The authentication process involves using a shared secret key. However, *Liao* does not teach or mention authenticating a mobile security module associated with a client or executing an authentication protocol for authenticating the mobile security module.

The portion of *Liao* at column 12, lines 36-55 states:

> To perform transactions in an authentic and secure session, each transaction must be assigned to a transaction ID. In one embodiment of the invention, a new transaction must have a new transaction ID and has to be in a trans-sequence, namely the transaction ID must be greater than any other completed and pending transaction IDs and less than 255 at the time the new transaction is started in the session, for example, transaction ID=12 for a current transaction, the next transaction ID from the client must be 13 or greater in order for the transaction to be accepted by the server. The constant 255 is the maximum number of transactions that can be performed in a valid session. If a transaction ID is smaller than what the session expects, the transaction is discarded without notice. If the transaction ID is greater than 255, a new session is automatically created to accommodate the corresponding transaction. All the data units related to transactions are encrypted with the session key created in the session creation process and the cipher used therein is either the client proposed cipher or the server proposed cipher.

Liao, column 12, lines 36-55.

This portion of *Liao* merely describes assigning a transaction ID to each transaction. A new transaction has a new transaction ID that is greater than any other completed and pending transaction ID. *Liao*'s teachings regarding a transaction ID does not disclose a mobile security module, executing an authentication process for authenticating a mobile security module, or authenticating a mobile security module by means of an authentication module. Thus, as shown above, neither Figures 4a and 4b nor the descriptions of Figures 4a and 4b disclose the execution step recited in claim 1.

Figure 5 of *Liao*, which is also cited by the Examiner, illustrates as follows:

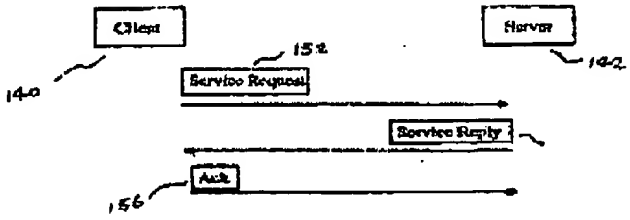


Fig. 5

Liao, Figure 5.

As shown above, figure 5 depicts a client sending a service request to a server. The figure illustrates a server sending a service reply to the client, and the client sending an acknowledgement to the server. Once again, a mobile security module associated with the client is not shown. Furthermore, the figure does not depict or disclose authenticating a mobile security module in any way.

The portion of *Liao* cited by the Examiner at column 12, line 56 to column 13, line 24 describes Figure 5 as follows:

> Referring to FIG. 5, there is shown a schematic diagram of a service transaction. The mobile client 140 initiates a Service Request (tSR) 152 to the server 142. A service transaction is typically involved in interaction with a service provider identified by a universal Resource Locator URL in a landline server, therefore the information in a tSR comprising URL and optional header that provides additional session information. Upon receiving the tSR 152, the server 142 processes the received tSR 152 to examine the sessionID and transaction ID therein. If the transaction ID is less than what it expects, the tSR 152 is discarded. In addition, the tSR 152 is discarded if the transaction ID in the received tSR 152 is greater that 255. As described above, for security reason, a maximum of 256 transactions is allowed in a session. If more than the allowed number of transaction occurs in one established session, a new session will be automatically initiated with the transaction ID being started from 0. Upon the successful examination of the service request tSR 152, the server 142 responds with a Service Reply (tSP) 154 that comprises a result in the form of digest of the URL service request and an optional header. Upon receiving the tSP 154 from the server 142, the client 140 sends the server 142 an acknowledge (ACK) 156 to commit the transaction if the result in the received tSP 154 is positive. Alternatively, the hand-held client can send the server a Cancel to abort the transaction. A typical example is that the client 140 requests to access information stored and identified by the URL as www.abc.com supported at the server 142, however, the URL in the tSR 152 is entered as www.abcd.com, the result in the

> tSP 154 returns a error message indicating the desired URL could not be found, otherwise the result in the tSP 154 shows the desired URL has been found, now it is up to the user of the client to determine if the client shall proceed with the tSP 156 or cancel to abort the current transaction to try a new or different URL.

Liao, column 12, line 56 to column 13, line 24.

This portion of *Liao* describes a service transaction in which a mobile client initiates a service request to a server. Upon receiving a service request, the server examines the session ID and transaction ID in the request, and responds with a service reply. The client sends the server an acknowledge signal to commit the transaction. Thus, *Liao* merely teaches a service transaction that does not involve a mobile security module of any kind. As shown above, neither Figure 5 nor the cited portion of the description provides any teachings regarding a mobile security module or an authentication protocol for authenticating a mobile security module.

Figure 6 of *Liao* illustrates as follows:

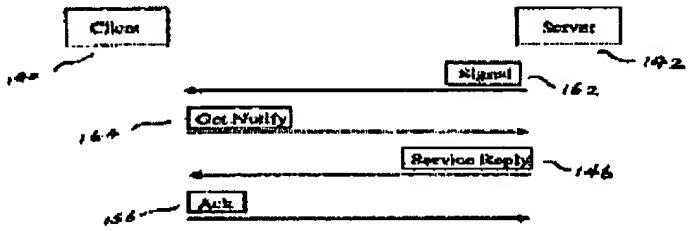


Fig. 6

Liao, Figure 6.

As can be seen, figure 6 is a diagram of a notification transaction. The figure depicts a client receiving a signal from a server. The client sends a get notify signal to the server. The server sends a service reply to the client. The client sends an acknowledgement to the server. The figure does not illustrate or depict a mobile security module or an authentication protocol for authenticating a mobile security module.

The cited portion of *Liao* describing Figure 6 states:

> Referring now to FIG. 6, there is shown a schematic diagram of a notification transaction. A notification transaction can be initiated by either the client 140 or the server 142. In the case of server initiation, the server 142 initiates the notification transaction by sending to the client 140 a signal data unit, or notification request (NR) 162, to inform the client 140 that there is a notification in pending in the server 142, such as an electronic mail, waiting for immediate attentions from the identified client. Upon receiving of the NS 162, the client 140

> sends a Get-Notify (GN) 164 to the server 142 and retrieves its notification contents such as alerts and emails. The server 142, as in the service transaction, replies with a tSR 146. The transaction is committed after an acknowledge signal (AS) 156 is sent to the server 142 and the server 142 receives it. In the case of the client notification, the client 140 initiates the notification transaction when it powers on or switches back to the data mode from voice mode by asking the server 142 if there is any notification in pending. If there is notification in pending, the client 140 handles the notification transaction as if a signal is received. The AS 156 may be piggybacked with a GN when multiple notification transactions are conducted sequentially. If there are multiple notifications are pending at the server 142, the optional header in the tSR 146 indicates that so that the client will automatically start another notification transaction.

Liao, column 13, lines 25-50.

This portion of *Liao* describes the notification transaction. *Liao* states that the notification transaction can be initiated by either a client or a server. In the case of a server initiation, the server sends a signal to a client. The client responds to the server with a Get Notify and retrieves its notification contents such as alerts and emails. The server sends a service reply. The transaction is committed after the server receives an acknowledge signal. However, Figure 6 and the cited portion *Liao* describing figure 6 do not teach a mobile security module or authenticating a mobile security module.

Regarding Figure 7, *Liao* illustrates as follows:

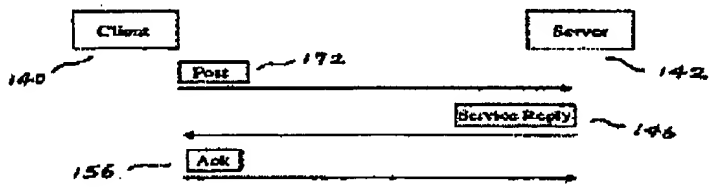


Fig. 7

Liao, Figure 7.

As shown above, *Liao* depicts a client sending a post signal to a server. The server sends a service reply signal to the client. And the client sends an acknowledge signal to the client. However, as can be seen, the figure does not depict a mobile security module or authenticating a mobile security module associated with a client.

The cited portion of the reference describing Figure 7 states:

> Referring now to FIG. 7, there is shown the post transaction. Post transaction is initiated by the mobile client 140. The post transaction is used for a mobile device to update information stored in a WWW service as specified in the URL. The client 140 sends a Post Request (PR) 172, which contains a URL, data for updating, and an optional header. The server 142 processes the PR 172 and responds to the client with a tSR 146. The result in the tSR 146 comes from the WWW service and normally indicates if information update is done. Upon receiving of the tSR 146, the client 140 sends the server 142 an AS 156 to commit the transaction. Alternatively, the mobile client 140 can send the server 142 a Cancel to abort the transaction.

Liao, column 13, lines 51-63.

Here, *Liao* states that a post transaction is used for a mobile device to update information stored in a WWW service. The client sends a post request which contains a URL to a server. The server responds with a tSR. Upon receiving the tSR, the client sends an acknowledge signal to the server to commit the transaction. Figure 7 and the cited portion of *Liao* do not teach or mention a mobile security module or authenticating a mobile security module. Furthermore, *Liao's* teachings regarding authenticating a client is not sufficient to disclose execution of an authentication protocol for authenticating the mobile security module associated with the client because *Liao* does not teach or even mention a mobile security module in any section of the reference.

3. Searching of the contents for further links

Moreover, *Liao* fails to teach "processing of the content requested for transmission and searching of the contents for other protected-access contents." *Liao* teaches:

> a link server, coupling the airnet to the landline network, for linking the first communication protocol to the second communication protocol, whereby the client can communicate with the server;

Liao, column 4, lines 23-26.

As shown above, *Liao* discloses a link server for linking a first and second communication protocol. However, merely disclosing a link server is not sufficient to teach **searching protected-access content for further links to other protected-access contents.** Moreover, *Liao* does not disclose searching protected content for links to other protected content in any other section of the reference. Therefore, *Liao* fails to teach "processing of the content requested for transmission and searching of the contents for other protected-access contents." Therefore, *Liao* fails to teach each and every feature of independent claim 1. *Liao* does not

teach each and every feature recited in amended independent claim 1. Therefore, *Liao* does not anticipate claim 1.

Dependent Claims 2-22 and 34

At least by virtue of their dependency on independent claim 1, dependent claims 2-22 are not anticipated by *Liao*. In addition, claims 2-22 recite additional features not taught or disclosed by *Liao*. For example, regarding claim 3, the Examiner believes *Liao* discloses the features recited in claim 3 at column 13, line 25 to line 50, which is quoted above. However, as discussed above, the cited portions of *Liao* merely teach a notification transaction between a server and a client. *Liao* does not teach sending a random number to an authentication module for authenticating a mobile security device, or generation of a digital signature which takes account of the identify number of the mobile security module, the random number and the key of the mobile security module, as is claimed in claim 3.

Regarding newly added claim 34, *Liao* does not teach a mobile security module is a chip card. As shown above, *Liao* does not teach a mobile security module in any section of the reference. Moreover, *Liao* does not teach or mention a chip card associated with the client or a chip card reader in any figure or section of the reference. Therefore, *Liao* fails to teach "wherein the mobile security module is a chip card and wherein the client includes a chip card reader," as is recited in newly added claim 34.

Independent Claims 23, 27, and 33

The examiner states on page 5 of the Office Action dated December 14, 2005 that:

> Regarding Claim 23 Liao teach and describe a method, in a client, for controlling access to protected contents (Fig.1-7), the method comprising: sending a request for protected content to a server; receiving an authentication applet and a random number from the server, wherein the random number is generated at the server; executing the authentication applet; sending, by the authentication applet, the random number to a mobile security module, wherein the mobile security module includes a cryptographic key and wherein the mobile security module gencrate3 a cryptographic signature based on the key and the random number; receiving, by the authentication applet, the cryptographic signature from the mobile security module; sending, by the authentication applet, the cryptographic signature to the server; and responsive to the server authenticating the cryptographic signature, receiving a session identifier from the server Fig. 1, 4- 7, and col.7 line 13 to line 32, and col.11 line to col.13 line 62).

Office Action dated December 14, 2005, page 5.

Independent claim 1 claims as follows:

> 23. A computer implemented method, in a client, for controlling access to protected contents using a mobile security module, the computer implemented method comprising:
>
> sending a request for protected content to a server;
>
> receiving an authentication applet and a random number from the server, wherein the random number is generated at the server;
>
> executing the authentication applet, wherein the authentication applet initiates communication with a mobile security module associated with the client;
>
> sending, by the authentication applet, the random number to the mobile security module, wherein the mobile security module includes a cryptographic key and wherein the mobile security module generates a cryptographic signature based on the key and the random number;
>
> receiving, by the authentication applet, the cryptographic signature from the mobile security module;
>
> sending, by the authentication applet, the cryptographic signature to the server; and
>
> responsive to the server authenticating the cryptographic signature, receiving a session identifier from the server.

Independent claims 27 and 33 recite similar subject matter. *Liao* does not teach executing the authentication applet or sending the random number to a mobile security module, as is claimed in claim 23.

Liao does not teach "executing the authentication applet, wherein the authentication applet initiates communication with a mobile security module associated with the client," as is claimed in amended claim 23. The Examiner believes that executing the authentication applet is taught by *Liao* at Figures 1, 4-7, and column 7, lines 13-32 and column 11, line 1 to column 13, line 62. The figures and cited portions of the text are shown above. As shown above, *Liao* merely discloses performing two rounds of authentication to authenticate a client and server using a shared secret encrypt key and a three message challenge/response exchange. The session creation involves sending/receiving a session request, a session reply, and a session complete signal. *Liao* also discloses a notification transaction and a post transaction. However, *Liao* does not does not teach or mention an authentication applet sent by the server or an applet that **initiates communication with a mobile security module** associated with the client. In fact, as discussed above, *Liao* does not disclose or mention a mobile security module in any figure or section of the reference. Thus, *Liao* fails to teach "executing the authentication applet, wherein

the authentication applet initiates communication with mobile security module associated with the client," as is recited in claim 23.

Furthermore, *Liao* does not teach "sending, by the authentication applet, the random number to the mobile security module, wherein the mobile security module includes a cryptographic key and wherein the mobile security module generates a cryptographic signature based on the key and the random number," as recited in amended independent claim 1. The Examiner believes this feature is disclosed by *Liao* at Figures 1, 4-7, and column 7, lines 13-32 and column 11, line 1 to column 13, line 62, which are shown and discussed above.

As was shown above with regard to independent claim 1, *Liao* fails to teach a mobile security module, as is recited in claim 23. Therefore, claim 23 is distinguishable over *Liao* for the same reasons discussed above with regard to independent claim 1. Moreover, the cited portions of *Liao* do not teach or mention sending a random number to a mobile security module, a mobile security module including a cryptographic key, or a mobile security module that generates a cryptographic signature based on the key and the random number. Thus, *Liao* fails to disclose "sending, by the authentication applet, the random number to the mobile security module, wherein the mobile security module includes a cryptographic key and wherein the mobile security module generates a cryptographic signature based on the key and the random number," as recited in claim 23.

Therefore, *Liao* fails to teach each and every feature recited in claim 23. Independent claims 27 and 33 recite similar subject matter addressed above with regard to independent claims 1 and 23. Therefore, independent claims 27 and 33 are also distinguishable over *Liao* for the same reasons set forth above with regard to claims 1 and 23. Thus, claims 23, 27, and 33 are not anticipated by *Liao*.

Dependent Claims 24-26, 28-32, and 35

At least by virtue of their dependency on independent claim 1, dependent claims 24-26, 28-32, and 35 are not anticipated by *Liao*. In addition, claims 24-26, 28-32, and 35 recite additional features not taught or disclosed by *Liao*. For example, regarding claims 25 and 29, the Examiner believes *Liao* discloses the mobile security module includes an individual number for the mobile security module and wherein the mobile security module generates the cryptographic signature based on the individual number at column 6, lines 25 to 54 and column 7, lines 14 to 62. *Liao* teaches:

> The communication protocol in the Internet 104 is HTTP that runs on TCP and controls the connection of an HTML Web browser to a Web server and the exchange of information therebetween. An extended version thereof, called HTTPS, provides encrypted authentication and session transmission between a client and a server. The communication protocol between the mobile device 106 and the link server 114 via the airnet 102 is Handheld Device Transport Protocol (HDTP), or Secure Uplink Gateway Protocol (SUGP), which preferably runs on User Datagram Protocol (UDP) and controls the connection of a HDML Web browser to a link server, where HDML stands for HandHeld Markup Language. The specification thereof and the HDTP specification are provided at http://www.wapforum.org http://www.openwave.com that are incorporated herein by reference. Further a reference specification entitled "Magellan SUGP Protocol" is incorporated herein by reference. The HDTP is a session-level protocol that resembles the HTTP but without incurring the overhead thereof and is highly optimized for use in mobile devices that have significantly less computing power and memory. Further it is understood to those skilled in the art that the UDP does not require a connection to be established between a client and a server before information can be exchanged, which eliminates the need of exchanging a large number of packets during a session creation. Exchanging a very small number of packets during a transaction is one of the desirous features for a mobile device with very limited computing power and memory to effectively interact with a landline device.

Liao, column 6, lines 25-54.

This cited portion of *Liao* teaches a Handheld Device Transport Protocol or Secure Uplink Gateway Protocol for controlling communication between a mobile device and a link server. However, such a protocol does not disclose a mobile security module associated with a client or an individual number for the mobile security module wherein the mobile security module generates a cryptographic signature based on the individual number. Thus, *Liao* fails to teach each and every feature of claims 25 and 29.

Regarding claims 31 and 35, *Liao* does not teach "wherein the mobile security module is a chip card and wherein the client includes a chip card reader," as is recited in dependent claims 31 and 35. The Examiner believes this feature is discloses by *Liao* at column 6, line 65-column 7, line 45, which states as follows:

> Although the user interface of the phone 120 is not shown in the figure, the mobile device 118, resembling a cellular phone, in FIG. 1 may be referenced thereto, in which referenced by 116 is a LCD screen and 118 is a key button pad, respectively. Through the screen 116 and the keypad 118 controlled by a user of the phone, the phone can be interactively communicated with a server through the airnet, link server and the Internet. According to one embodiment of the present invention, compiled and linked processes of the present invention are stored in

> ROM 122 as a client module 124 and support module 126. Upon activation of a predetermined key sequence utilizing the keypad 118, a physical layer processor or microcontroller 118, initiates a session communication to the server using the module 124 in the ROM 122.
>
> To establish a secured communication between a client and a server, an authentication process must be conducted first to ensure that only interested parties are actually in the communication therebetween. The process is complete through two rounds of independent authentication, one being the client authenticated by the server, referred to as client authentication, and the other being the server authenticated by the client, referred to as server authentication. Further each authentication is completed in two separate steps for high grade of security, which will be described in detail below. The success of the mutual authentication processes provision an evidence that the two communicating parties possesses a valid shared secret encrypt key through a mutual decryption and a challenge/response mechanism. The mutual decryption mechanism comprises the steps of mutually recovering encrypted messages from two involved communicating parties. The challenge/response mechanism, referred to as nonce verification, verifies a predetermined relationship between a sent nonce and a received derivative thereof.

Liao, column 6, line 65 to column 7, line 45.

Here, *Liao* describes a mobile phone that can communicate with a server through an airnet. An authentication process can be conducted to establish a secure communication between a client and server. The process is complete through two rounds of independent authentication for authenticating a server by a client and authenticating a client by the server. Although *Liao* describes one possible authentication process using a shared secret encrypt key and a challenge/response mechanism for authenticating a client that can be a mobile phone, *Liao* does not disclose or mention a mobile security module or a chip card associated with the client. Moreover, *Liao* does not mention authenticating a chip card associated with a client, a chip card having a protected area for storing a key, or a chip card reader. Therefore, the cited portion of the reference fails to teach each and every feature of claims 31 and 35.

As shown above with regard to claims 1, 23, 27, and 33, *Liao* does not teach a mobile security module in any section or figure of the reference. Likewise, *Liao* does not teach or mention a chip card associated with the client in any figure or any section of the reference. Thus, *Liao* fails to teach "wherein the mobile security module is a chip card," as is recited in newly added claim 34. Therefore, the rejection of claims 1-5, 7-9, 12-14, and 23-33 under 35 U.S.C. § 102 has been overcome.

Furthermore, *Liao* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. *Liao* actually teaches away from the presently claimed invention because it teaches a process based on a shared secret encrypt key and a challenge/response mechanism rather than authenticating a client based on a mobile security module associated with the client as in the presently claimed invention. Absent the examiner pointing out some teaching or incentive to implement *Liao* and utilization of a mobile security module card for authenticating a client, one of ordinary skill in the art would not be led to modify *Liao* to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify *Liao* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

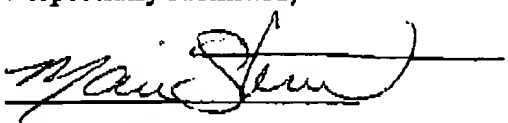
III. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: June 27, 2006

Respectfully submitted,



Mari Stewart
Reg. No. 50,359
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants